(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 43 310 A 1**

(51) Int. Cl.[7]:
H 04 L 9/32
G 06 F 13/00

(21) Aktenzeichen: 100 43 310.3
(22) Anmeldetag: 17. 8. 2000
(43) Offenlegungstag: 22. 3. 2001

DE 100 43 310 A 1

Mit Einverständnis des Anmelders offengelegte Anmeldung gemäß § 31 Abs. 2 Ziffer 1 PatG

(71) Anmelder:
Rozek, Werner, Prof. Dr.-Ing. Dipl.-Ing., 98593 Floh-Seligenthal, DE

(72) Erfinder:
gleich Anmelder

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur eindeutigen und fälschungssicheren Zustellung von elektronischen Daten über Kommunikationsnetze

(57) Verfahren zur eindeutigen und fälschungssicheren Zustellung von elektronischen Daten über Kommunikationsnetze, die von einem Sender zu einem Empfänger übertragen werden, ist dadurch gekennzeichnet, dass ein globaler Raum, ein Identitätsraum, Identitätsbezugspunkte, Identitätspunkte, ein Verschlüsselungspunkt und Raumbezugspunkte sowie Vorgaben vorhanden sind und eine Vorgabe zu nicht voraussagbaren zufälligen Zeiten verändert wird. Die Sender und Empfänger generieren aus den Vorgaben Räume, Bezugsflächen, Bezugspunkte, ermitteln anhand von Identitätspunkte in bezug auf einen Identitätsraum seine Identität, bestimmen Informationen zu den Lagen der Identitätspunkte und eines Verschlüsselungspunktes zu Bezugspunkten, verschlüsseln die zusendenden und entschlüsseln die empfangenen Daten plus Zusatzinformationen anhand des Verschlüsselungspunktes.

DE 100 43 310 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur eindeutigen und fälschungssicheren Zustellung elektronischer Daten über Kommunikationsnetze, die von einem Sender zu einem Empfänger übertragen werden.

Beim Verleih oder Verkauf und bei der Zustellung elektronischer Daten über ein Kommunikationsnetz wie z. B. das Internet ist die eindeutige, nicht manipulierbare und fälschungssichere Zustellung einer elektronischen Ware existenzielle Voraussetzung für diese Dienstleistung. So können als elektronische Daten z. B. Videodaten, Audiodaten, Software, elektronische Zeitungen und Bücher oder anderer Daten von einem Provider im Netz angeboten werden. Ein Kunde wählt seine elektronische Ware und lädt diese Ware vom Providersystem in sein Kundensystem. Ein bedeutender Anwendungsfall stellt die Internet-Videothek dar. Bei konventionellen Videotheken besuchen Kunden die Räume der Videothek, wählen einen Videofilm oder mehrere Filme und leihen diese für einen Zeitraum aus. Je nach Ausleihdauer wird eine entsprechende Gebühr erhoben. Eine Kopierung des Videofilms ist über die Gesetzgebung verboten. Zur Abwicklung dieser Verfahrensweise innerhalb der elektronischen Medien ist ein Verfahren erforderlich, das eine eindeutige und fälschungssichere Zustellung ermöglicht.

Aus WO 9953624 ist ein GPS Signalzugriffsystem bekannt, das den Zugriff autorisierter Empfänger auf z. B. Videodaten, Audiodaten, Internetdaten oder Datensignale, die von einer Zentralen ausgesandt werden, ermöglicht. Ein Merkmal dieser Lösung ist, das die Kundensignalzugriffsteuerung nur autorisiert zugreifen kann, wenn sie autorisierend lokalisiert ist, wobei ein GPS-Empfänger benutzt wird. Das GPS-Signalzugriffsystem benutzt die GPS-Positionsdaten für die Autorisierung an einem einzelnen Ort. Das Signalzugriffsystem hat weiterhin eine zentrale Zugriffssteuerung, die ein GPS- Empfänger verwendet und Positionsdaten liefert, die über ein Übertragungsmedium zu den Kunden übertragen werden. Positionsdaten der Kundenzugriffsteuerung und der zentralen Steuerung werden für den autorisierten Zugriff auf gesendete Signale verwendet.

Die GPS-Signalzugriffsteuerung erlaubt der Zentralen die Lokalisierung einer Kundenzugriffsteuerung und deren Autorisierung für den Zugriff auf die gewünschten, von einer Zentralen ausgesandten Daten. Ein Nachteil dieser Lösung liegt darin, dass ein GPS und ein weiteres Zentralsystem benötigt wird und dass nicht jeder Empfänger, der an ein Übertragungsmedium angeschaltet ist, jeden Sender, der an dem selben Übertragungsmedium angeschaltet ist, fälschungssicher Daten übertragen kann. Nicht das einzelne Kundensystem steht bei der Lösung im Mittelpunkt, sondern die Sendung von Daten einer Zentralen an einer Vielzahl von Kunden.

Die Aufgabe der Erfindung besteht darin, ein Verfahren zur eindeutigen und fälschungssicheren Zustellung elektronischer Daten über Kommunikationsnetze zu schaffen, wobei folgende Zielstellungen verfolgt werden:

- eindeutige und fälschungssichere Identifikation des Kunden
- eindeutige und nicht beeinflussbare Zustellung des elektronischen Mediums
- nichtkopierbare Bereitstellung des elektronischen Mediums für eine Ausleihdauer
- eindeutige Bereitstellung des elektronischen Mediums bei Kauf nur für das jeweilige Kundensystem

Weitere Ziele der Erfindung sind, trotz öffentlichem Verfahren keine Manipulationen an den Identitäten des Kunden

bzw. Providers zu zulassen, die eindeutigen Zustellung und Bereitstellung in bezug auf die Ausleihe und deren Ausleihdauer bzw. den Kauf des elektronischen Mediums zu ermöglichen.

Die Aufgabe wird erfindungsgemäß durch das Verfahren nach der Lehre der Ansprüche gelöst.

Im folgenden wird die Erfindung anhand der **Fig.** 1 bis 17 näher erläutert. Die Zeichnungen stellen bevorzugte Ausführungsbeispiele der Erfindung dar. Es zeigen

Fig. 1 eine schematische Darstellung einer Anordnung zur Sendung der Vorgaben,

Fig. 2 ein Blockbild eines Sende- und Empfangsgeräts,

Fig. 3 ein Blockbild einer Identitätskarte (ID-Card),

Fig. 4 die Verfahrensschritte auf der ID-Karte,

Fig. 5 den Aufbau eines Kartendatentelegramms KDT1,

Fig. 6 die Verfahrenschritte zum Verschlüsseln der Daten,

Fig. 7 die Bestimmung eines Verschlüsselungspunktes,

Fig. 8 die Bestimmung aller Identitätspunkte einer Person in einem Identitätsraum IR,

Fig. 9 die Ermittlung von Informationen zu den Lagen der zu übertragenden Identitätspunkte in Form von Abstandsvektoren,

Fig. 10 die Ermittlung von Informationen zu den Lagen der zu übertragenden Identitätspunkte in Form von Einheitsvektoren,

Fig. 11 den Aufbau eines Kartendatentelegramms KDT2,

Fig. 12 ein Blockbild eines Telegramm-Schlüssel-Controllers,

Fig. 13 den Aufbau eines Vorgabendatentelegramms VDT1,

Fig. 14 den Aufbau der Datentelegramme DT1 und DT2 in einer ersten Ausführungsart,

Fig. 15 den Aufbau der Datentelegramme DT1 und DT2 in einer zweiten Ausführungsart,

Fig. 16 den Aufbau der Speicherdatentelegramme SDT1 und SDT2,

Fig. 17 die Bestimmung der zu übertragenden Identitätspunkte im Telegramm-Schlüssel-Controller,

In **Fig.** 1 sind dargestellt: ein Vorgabensender **12**, ein Sende-Empfangsgerät **131**, ein Sende-Empfangsgerät **132**, einen Satelliten **11** und ein Übertragungsmedium **15**. **Fig.** 2 zeigt das Blockbild eines Sende-Empfangsgerätes **131**. Das Sende-Empfangsgerät **131** besteht aus einer ID-Card **3**, einem Telegrammempfänger **21**, einem Telegrammsender **22**, einem Telegramm-Schlüssel-Controller **23** und aus einem Datenspeicher **24**.

Fig. 3 stellt einen internen Aufbau der ID-Card dar. Im einzelnen sind auf der ID-Card enthalten: ein Modul **31** zur Eingabe eines Kartenbezugspunktes CBP_e, ein Modul **32** zur Speicherung eines geheimen Kartenbezugspunktes CBP_g, eines geheimen Kartenidentitätspunktes CIP_g, eines geheimen Personenidentitätspunktes PIP, eines öffentlichen Identitätspunktes $IP_ö$, ein Modul **33** zur Bestimmung des Kartenbezugspunktes CIP, ein Modul **34** zum Vergleich des ermittelten Kartenidentitätspunktes CIP mit dem geheimen Kartenidentitätspunkt CIP_g, ein Modul zur Ermittlung der Kartenbezugspunkte KBP_{i1}, KBP_{i2}, des Ursprungs UVR_i des Verschlüsselungsraumes VR in der i-ten Lage, des Ursprungs UVR_{i+1} des Verschlüsselungsraumes in der (i+1)-ten Lage des Verschlüsselungsraumes VR in einem globalen Raum, des Ursprunges UIR_i des Identitätsraumes, des Verschlüsselpunktes VP_i, des Datenabstandes ADB_i für den Datentausch, des Zusatzinformationsanfangspunktes ZIA_i, des Datenabstandes der Zusatzinformation AZI_i, ein Modul **36** zur Speicherung der Ortvektoren $OVKBP_{i+1,2}$, $OVKBP_{i+1,1}$ der Kartenbezugspunkte $KBP_{i+1,2}$, $KBP_{i+1,1}$, und des Ortvektors $OVUVR_{i+1}$ des Ursprungspunktes UVR_{i+1}, ein Modul **37** zur Speicherung der Ortvektoren $OVKBP_{i,2}$,

$OVKBP_{i,1}$ der Kartenbezugspunkte $KBP_{i,2}$, $KBP_{i,1}$, und des Ortvektors $OVUVR_i$ des Ursprungspunktes UVR_i ein Modul **38** zur Ermittlung der Informationen zu den Lagen der zu übertragenden Identitätspunkte IDP und $IP_{ö}$, ein Modul **39** zur Speicherung des Ortvektors $OVUVR_{i-1}$, ein Kartentelegrammempfänger **310** und ein Kartentelegrammsender **311**.

Die auf der ID-Card ausgeführten Verfahrensschritte sind aus **Fig.** 4 erkennbar. **Fig.** 5 zeigt den Aufbau des Kartendatentelegramms KDT1. Das Kartendatentelegramm KDT1 wird von einem Kartentelegramm-Schlüssel-Controller **231** des Telegramm-Schlüssel-Controllers **23** gesendet. Das Kartendatentelegramm KDT1 setzt sich aus zwei Telegrammteilen zusammen. Der erste Telegrammteil enthält den Einheitsvektor der Geraden, die durch den Verschlüsselungspunkt VP und dem Kartenbezugspunkt KBP_{i1} geht, und den Einheitsvektor der Geraden, die durch den Verschlüsselungspunkt VP und dem Kartenbezugspunkt KBP_{i2} verläuft. Der Telegrammteil **2** enthält die Ortvektoren $OVKBP_{i,2}$, $OVKBP_{i,1}$ der Kartenbezugspunkte $KBP_{i,2}$, $KBP_{i,1}$, und die Ortvektoren $OVUVR_i$, $OVUVR_{i+1}$ des Ursprungspunktes UVR_i , UVR_{i+1}, den Ortsvektor des Ursprungs vom Identitätsraum sowie eine Vielzahl von Zufallszahlen Z_{si}. Die Zufallszahlen werden von einem Zufallsgenerator des Kartentelegramm-Schlüssel-Controllers erzeugt und dienen in Verbindung mit dem Datentausch zur Verschleierung der Zusatzinformationen. Die Verfahrensschritte des Datentausches im Telegrammteil **2** sind in **Fig.** 6 an einem Beispiel demonstriert. Nur unter Kenntnis der unverschlüsselten Einheitsvektoren und der verschlüsselt übertragenen Bezugspunkte ist die Bestimmung eines Verschlüsselungspunktes überhaupt möglich.

In **Fig.** 7 ist die Bestimmung des Verschlüsselungspunktes im globalen Raum dargestellt. Durch das Antragen von den Ortvektoren $OVKBP_{i1}$, $OVKBP_{i2}$ im Ursprung des globalen Raums sind die Lagen der Kartenbezugspunkte KBP_{i1}, KBP_{i2} fixiert. Mit dem Antragen der Einheitsvektoren $EV_{VPKBPi1}$ Und $EV_{VPKBPi2}$ in den Kartenbezugspunkten KBP_{i1} und KBP_{i2} ist der Verschlüsselungspunkt durch den Schnittpunkt beider Einheitsvektoren bestimmt. Die Lotbildungen auf die Verschlüsselungsbezugsebenen des Verschlüsselungsraumes ergeben die für die Entschlüsselung des Telegrammteils **2** benötigten Informationen. **Fig.** 8 zeigt den geheimen Personenidentitätspunkt PIP, der mit Hilfe einer Transformation einer Personenkennzahl in den Identitätsraum integriert worden ist. Weiterhin sind der Kartenbezugspunkt CBP_e, der geheimen Kartenbezugspunkt CBP_g, der geheimen Kartenidentitätspunkt CIP_g, der beim Empfänger bekannt werdende Identitätspunktes $IP_{ö}$, die Ortvektoren $OV_{IPö}$ und OV_{IDP} sowie der Abstandsvektor AV_{PIPCIP} im Identitätsraum dargestellt.

Durch die Eingabe des einer Person zugeordneten Kartenbezugspunktes CBP_e ist die Karte nur in Verbindung mit der Person nutzbar.

Der Kartenbezugspunkt CBP_e kann eine PIN-Nummer oder der Fingerabdruck dieser Person sein. Die Lage des geheimen Kartenidentitätspunktes ergibt sich aus dem Schnittpunkt der Lotgeraden, die in den Kartenbezugspunkten errichtet wurden. Die Prüfung der Gültigkeit des berechneten Kartenbezugspunktes erfolgt im Vergleich mit dem gespeicherten geheimen Kartenidentitätspunkt CIP_g. Sind beide gleich, so ist die Karte für die Person gültig. Die Ermittlung des Abstandsvektors AV_{PIPCIP}, deren Verschiebung in den Punkt $IP_{ö}$ ergibt den auszutauschenden geheimen Identitätspunkt IDP.

Der beim Empfänger bekannt werdende Identitätspunkt $IP_{ö}$ ist mit Hilfe einer Transformation vorteilhaft der Adresse der Person zugeordnet.

In **Fig.** 9 sind im globalen Raum die Lage des Identitätsraumes IR, die Lagen des Identitätspunktes IDP und $IP_{ö}$, die Kartenbezugspunkte KBP_{i1}, KBP_{i2}, deren Ortvektoren $OVKBP_{i1}$, $OVKBP_{i2}$ und die Abstandsvektoren $AV_{IPöKBPi2}$, $AV_{IDPKBPi1}$ abgebildet.

Fig. 10 zeigt im globalen Raum die Lage des Identitätsraumes IR, die Lagen des Identitätspunktes IDP und $IP_{ö}$, die Kartenbezugspunkte KBP_{i1}, KBP_{i2}, die Einheitsvektoren $EV_{IPöKBPi1}$, $EV_{IPöKBPi2}$, $EV_{IDPKBPi1}$ und $EV_{IDPKBPi2}$.

Durch die Übertragung der vier Einheitsvektoren im Kartendatentelegramm KDT2 bleiben die auszutauschenden Identitätspunkte IDP und $IP_{ö}$ geheim. Die Endpunkte IDP und $IP_{ö}$ sind nur relativ bekannt, weil außerhalb der ID-Card bzw. des Kartentelegramm-Schlüssel-Controllers die Kartenbezugspunkte verborgen bleiben.

Der Aufbau des Kartendatentelegramms KDT2 ist in der **Fig.** 11 beschrieben. Der Ortvektor $OVUVR_{i-1}$ ist in dem dargestellten Beispiel im Telegramm integriert. Eine vorteilhafte Lösung wäre auch die Sendung des Ortvektors über einen eigenen Ausgang. Damit könnte der Kartentelegramm-Schlüssel-Controller die Kommunikation eröffnen. Im dargestellten Fall sendet die ID-Card in bestimmten Abständen das Kartendatentelegramm KDT2 aus.

In **Fig.** 12 ist der Telegramm-Schlüssel-Controller (TSC) gezeichnet. Der Telegramm-Schlüssel-Controller **23** besteht aus einem Kartentelegramm-Schlüssel-Controller **231**, einem Vorgabentelegramm-Schlüssel-Controller **232**, einem Datentelegramm-Schlüssel-Controller **233** und einer Schlüssel-Protokollierungs-Einheit **234**. Der Controller **231** generiert das Kartendatentelegramm KDT1 für die Sendung zur ID-Card **3**. Er fragt den Ortvektor $OVUVR_{i-1}$ an der ID-Card ab, schlussfolgert daraus auf die Kartenbezugspunkte, bestimmt mit einem Zufallsgenerator den Datenabstand ADB_i für den Datentausch, den Anfangspunkt ZIA_i der Zusatzinformation im KDT1, den Datenabstand AZI_i der Zusatzinformation und bestimmt die Einheitsvektoren $EV_{VPKBPi1}$, $EV_{VPKBPi2}$ für den Verschlüsselungspunkt VP in bezug auf die zur Zeit gültigen Kartenbezugspunkte KBP_{i1}, KBP_{i2}. Mit einem Zufallsgenerator erzeugt der Kartentelegramm-Schlüssel-Controller eine Vielzahl von Zufallszahlen Z_S. Bei 5 Zusatzinformationen ist der zehnfache Wert an Schlüsselzahlen eine geeignete Größenordnung. Aus dem empfangenen Kartendatentelegramm KDT1 selektiert der Controller **231** die Einheitsvektoren. In Zusammenarbeit mit dem Vorgabentelegramm-Schlüssel-Controllers **232** werden die Einheitsvektoren durch Vektorsumme in den Kartenbezugspunkten, wie in **Fig.** 10 oder 17 dargestellt, angetragen. Damit sind dem Telegramm-Schlüssel-Controller **23** die Identitätspunkte IDP und $IP_{ö}$ bekannt.

In **Fig.** 13 ist der Aufbau des Vorgabendatentelegramms VDT1 abgebildet. Das Vorgabendatentelegramm ist ebenfalls zweigeteilt.

Im ersten Telegramteil werden ein Controller-Schlüssel CS und die Einheitsvektoren $EV_{CVPCBPi1}$, $EV_{CVPCBPi2}$ übersandt. In dem zweiten Telegrammteil sind mindestens die Ortvektoren zweier Lagen des Ursprungspunktes des Verschlüsselungsraumes, des Ursprungspunktes des Identitätsraumes, zweier Kartenbezugspunkte, zweier Controllerverschlüsselungsbezugspunkte, von sechs globalen Raumbezugspunkten und Zufallszahlen enthalten, wobei die Daten im zweiten Telegrammteil in Abhängigkeit von den im Verschlüsselungspunkt enthaltenen Informationen verschlüsselt sind. Die Einheitsvektoren sind Vektoren der Geraden mit den Punkten des Verschlüsselungspunktes und je einem Controllerverschlüsselungsbezugspunkt im globalen Raum. Der Controllerschlüssel dient der Auswahl geheimer Controllerbezugspunkte, die nur im Vorgabentelegramm-Schlüssel-Controller bekannt sind.

Fig. 14 zeigt den Aufbau der Datentelegramme DT1 und DT2. Auch diese Datentelegramme sind zweigeteilt. Im ersten Teil stehen wiederum Einheitsvektoren $EV_{CVPGBPik}$ von den Geraden, die durch den Controllerverschlüsselungspunkt CVP_i und dem globalen Raumbezugspunkt GBP_k festgelegt sind. In diesem Fall sind sechs Einheitsvektoren benutzt. Dies ist erforderlich, weil bei der Sendung sich die Lage zweier globaler Raumbezugspunkte verändern kann. Damit der Empfänger z. B. eines Providersystems **132** trotz Änderung der globalen Raumbezugspunkte den Verschlüsselungspunkt eindeutig erkennt, müssen die verbleibenden Lagen unverändert bleiben. Durch Mehrheitsentscheid in bezug auf die Schnittpunkte der Einheitsvektoren, die in den globalen Raumbezugspunkte angetragen wurden, wird der Verschlüsselungspunkt VP ermittelt. Mit der Kenntnis des Verschlüsselungspunktes VP sind die Entschlüsselungsdaten ADB_i, ZIA_i und AZI_i ermittelt. Nach dem Datentausch und der Selektion der Zusatzinformationen sind dem Empfänger alle Daten bekannt. Mit dem Identitätspunkt kann das Sende-Empfangsgerät **132** als Providersystem in Verbindung mit einer Adressen-CD die Anschrift des Absenders eindeutig ermitteln.

In **Fig.** 15 ist eine zweite Ausführungsart der Datentelegramme DT1 und DT2 abgebildet. Wie aus dem Bild erkennbar, werden die Einheitsvektoren für die Geraden des Identitätspunktes IDP und der globalen Raumbezugspunkte gebildet. Mit dieser Lösung existieren für jedes Sende-Empfangsgerät **131** unterschiedliche Einheitsvektoren.

Fig. 16 zeigt einen Aufbau der Speicherdatentelegramme SDT1 und SDT2. Die Merkmale der Telegramme sind eine Datenverwaltungsnummer $DTLN_j$ und der nach den Informationen des Verschlüsselungspunktes verschlüsselte Datenstrom.

Im Anwendungsfall einer Internetvideothek steckt ein Kunde seine ID-Card in das Sende-Empfangsgerät **13**, im weiteren als Kundensystem **131** genannt. Der Kartentelegramm-Schlüssel-Controller erkennt anhand des Ortsvektors $OVUVR_{i-1}$ die gültigen Kartenbezugspunkte, sendet zur ID-Card neue Kartenbezugspunkte mit dem Kartendatentelegramm KDT1. Die ID-Card sendet nach der Bestimmung der Einheitsvektoren der Identitätspunkte IDP und $IP_ö$ das Kartendatentelegramm KDT2 zurück. In dem Datentelegramm-Schlüssel-Controller werden die Einheitsvektoren der Identitätspunkte in bezug auf die Raumbezugspunkte RBP, die Einheitsvektoren des Verschlüsselungspunktes in bezug auf die Identitätspunkte IDP und $IP_ö$ generiert, die Daten mit den Informationen des Verschlüsselungspunktes neu verschlüsselt und mit dem Datentelegramm DT2 zum Providersystem **132** der Internetvideothek gesendet. Im Providersystem **132** werden die geheimen Identitätspunkte in bezug auf die globalen Raumbezugspunkte bestimmt. Nach Kenntnis der Lagen von IDP und $IP_ö$ wird der Verschlüsselungspunkt durch das Antragen (Vektorsummenbildung) der Einheitsvektoren EV_{IDPVP} und $EV_{IPöVP}$ und Schnittpunktbestimmung ermittelt. Aus den Koordinateninformationen des Verschlüsselungspunktes werden die Verschlüsselungsdaten ADB, ZIA und AZI generiert und damit die Daten entschlüsselt. Nach Auswahl eines Videofilms bildet das Providersystem **132** mit Hilfe eines Zufallsgenerators die Verschlüsselungsdaten ADB, ZIA und AZI. Zusätzlich werden Informationen wie Ausleihdauer und/oder Kosten und/oder Providerbezugspunkte und anderes mehr übermittelt. Die Daten des Videofilmes und die Zusatzinformationen werden verschlüsselt und mit den Einheitsvektoren der Identitätspunkte des Providersystems in bezug auf die Raumbezugspunkte RBP und den Einheitsvektoren des Verschlüsselungspunktes VP in bezug auf die Identitätspunkte IDP und $IP_ö$ des Providersystems gemeinsam im Datentelegramm DT1 zum Kundensystem **131** gesendet. Dort angekommen, selektiert der Datentelegramm-Schlüssel-Controller **233** die Einheitsvektoren und daraus die Identitätspunkte des Providersystems. Der Schnittpunkt der Einheitsvektoren EV_{IDPVP} $EV_{IPöVP}$ ergibt den Verschlüsselungspunkt im globalen Raum. Die Lage des Verschlüsselungsraumes im Verschlüsselungsraum wird durch den Ortvektor des Ursprungpunktes des Verschlüsselungsraumes bestimmt. Nach der Ermittlung von ADB, ZIA und AZI erfolgt die Selektion der Zusatzinformation aus den Daten und deren Abspeicherung in der Schlüssel-Protokollierungseinheit **234**. Die verschlüsselten Daten werden im Datenspeicher **24** gespeichert. Bei Nutzung der Daten, d. h. beim Ansehen des Videofilmes werden die Daten entschlüsselt. Ist die Ausleihzeit abgelaufen, so werden die Verschlüsselungsinformationen aus der Einheit **234** gelöscht.

Dieser Ablauf ist auch bei dem Verkauf von Software vorteilhaft anwendbar. Mit dem verschlüsselten Speicher der Software, und der geheimen Abspeicherung der Entschlüsselungsinformationen in dem Zielgerät kann keine Raubkopie erstellt werden. Ein Kopieren erfolgt nur mit den verschlüsselten Daten.

Patentansprüche

1. Verfahren zur eindeutigen und fälschungssicheren Zustellung von elektronischen Daten über Kommunikationsnetze, die von einem Sender zu einem Empfänger übertragen werden, ist **dadurch gekennzeichnet**,
   - dass in mindestens einem globalen Raum (GR) mindestens ein Identitätsraum (IR) und/oder eine Identitätsbezugsfläche und/oder einen Identitätsbezugspunkt, mindestens ein Verschlüsselungsraum (VR) und/oder eine Verschlüsselungsbezugsfläche und/oder einen Verschlüsselungsbezugspunkt und mindestens ein Bezugsraum (BR) und/oder eine Bezugsfläche und/oder einen Raumbezugspunkt vorhanden sind,
   - dass für die Räume und/oder Bezugsflächen und/oder Raumbezugspunkte Vorgaben existieren, die Eigenschaften über die Räume und 1 oder Bezugsflächen und/oder Raumbezugspunkte enthalten,
   - dass mindestens eine Eigenschaft in bezug auf einen Raum und/oder eine Bezugsfläche und/oder einen Raumbezugspunkt nicht voraussagbar zu zufälligen Zeiten verändert wird,
   - dass die Vorgaben von einem Vorgabensender bereitgestellt werden,
   - dass die Sender und Empfänger aus den Vorgaben die Räume und/oder Bezugsflächen und/oder Bezugspunkte in dem globalen Raum oder in den globalen Räumen generieren,
   - dass der Sender seine Identität anhand mindestens eines Identitätspunktes in bezug auf mindestens einen Identitätsraum und/oder einer Identitätsbezugsfläche und 1 oder einen Identitätsbezugspunkt ermittelt,
   - dass der Sender mindestens eine Information zur Lage des Identitätspunktes oder zu den Lagen mehrerer Identitätspunkte zu mindestens einem Bezugspunkt bestimmt,
   - dass der Sender mindestens einen Sendeschlüssel anhand mindestens eines Verschlüsselungspunktes in bezug auf mindestens einen Verschlüsselungsraum und/oder einer Verschlüsselungsbezugsfläche und/oder Verschlüsselungsbezugspunkt bildet,

– dass der Sender mindestens eine Information zur Lage des Verschlüsselungspunktes oder zu den Lagen mehrerer Verschlüsselungspunkte zu mindestens einem Bezugspunkt bestimmt,
– dass der Sender die zu übertragenden Daten nach dem Sendeschlüssel verschlüsselt,
– dass der Sender mindestens eine der Informationen zu den Lagen und die, mit dem Sendeschlüssel, verschlüsselten Daten sendet,
– dass der Empfänger aus den empfangenen Informationen die Lage des Identitätspunktes bzw. die Lagen der Identitätspunkte und die Lage des Verschlüsselungspunktes bzw. die Lagen der Verschlüsselungspunkte in bezug auf den Bezugspunkt oder auf die Bezugspunkte ermittelt,
– dass der Empfänger anhand des Identitätspunktes bzw. anhand der Identitätspunkte die Identität des Senders bestimmt,
– dass der Empfänger anhand des Verschlüsselungspunktes bzw. anhand der Verschlüsselungspunkte den Sendeschlüssel generiert, die verschlüsselten Daten anhand des Sendeschlüssels entschlüsselt werden.

2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die Koordinaten des Verschlüsselungspunktes den Anfangspunkt der zuintegrierenden Zusatzinformationen, einen Abstandswert der zutauschenden Daten, einen Abstandswert der Zusatzinformationen im zu übertragenden Datenstrom charakterisieren.

3. Verfahren nach Anspruch 2 dadurch gekennzeichnet, dass die Abstandswerte und der Anfangspunkt durch einen Zufallsgenerator bestimmt werden.

4. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass mindestens ein für den Austausch vorgesehener Identitätspunkt und mindestens ein geheimer nicht für den Austausch vorgesehener Identitätspunkt im Identitätsraum existieren.

5. Verfahren nach den Ansprüchen 1 und 4 dadurch gekennzeichnet, dass die Identität des Senders anhand mindestens einen für den Austausch vorgesehenen Identitätspunkt festgestellt wird.

6. Verfahren nach Anspruch 5 dadurch gekennzeichnet, dass die Identität des Senders anhand eines für den Austausch vorgesehenen Identitätspunktes am Empfänger bekannt wird, wobei mindestens ein für den Austausch vorgesehener Identitätspunkt im Empfänger geheim benutzt wird.

7. Verfahren nach Anspruch 6 dadurch gekennzeichnet, dass dem beim Empfänger bekannt werdenden Identitätspunkt eine Adresse zugeordnet ist.

8. Verfahren nach Anspruch 7 dadurch gekennzeichnet, dass der im Empfänger bekannt werdende Identitätspunkt in Form seiner Adresse bekannt gemacht wird.

9. Verfahren nach Anspruch 4 dadurch gekennzeichnet,
– dass die Lage eines der geheimen Identitätspunkte im Identitätsraum durch den Schnittpunkt mindestens zweier Lotgeraden ermittelt wird,
– dass jede Lotgerade von einem Lotbezugspunkt einer geheimen Lotbezugsebene ausgeht,
– dass einer der Lotbezugspunkte für alle Personen bis auf eine Person geheim ist und jeder weitere Lotbezugspunkt geheim ist.

10. Verfahren nach den Ansprüchen 4 bis 7 dadurch gekennzeichnet, dass die Lage eines zweiten geheimen Identitätspunktes im Identitätsraum durch eine Transformation aus einer Personenkennzahl sich bestimmt.

11. Verfahren nach den obigen Ansprüchen dadurch gekennzeichnet,
– dass ein Abstandsvektor zwischen den nicht für den Austausch vorgesehenen Identitätspunkten ermittelt wird,
– dass dieser in dem für den Austausch vorgesehenen und im Empfänger bekannt werdenden Identitätspunkt im Identitätsraum angetragen wird, wobei der Endpunkt der für den Austausch vorgesehene geheime Identitätspunkt ist.

12. Verfahren nach Anspruch 1 dadurch gekennzeichnet,
– dass die Informationen zu den Lagen der Identitätspunkte und zu den Lagen der Verschlüsselungspunkte Abstandsvektoren zu mehr als einem Bezugspunkt sind,
– dass zur Ermittlung jedes Identitätspunktes und jedes Verschlüsselungspunktes der Abstandsvektor in den Bezugspunkten angetragen werden.

13. Verfahren nach Anspruch 1 dadurch gekennzeichnet,
– dass die Informationen zu den Lagen der Identitätspunkte und zu den Lagen der Verschlüsselungspunkte Einheitsvektoren in bezug auf die Bezugspunkte sind,
– dass zur Ermittlung jedes Identitätspunktes und jedes Verschlüsselungspunktes die jeweiligen Einheitsvektoren in den Bezugspunkten angetragen werden und die Schnittpunkte den gesuchten Identitätspunkt oder die gesuchten Identitätspunkte bzw. den Verschlüsselungspunkt oder die Verschlüsselungspunkte ergeben.

14. Verfahren nach Anspruch 1 dadurch gekennzeichnet,
– dass alle Identitätsräume im globalen Raum jeweils einen eindeutigen Bezug zu allen Bezugsräumen (BR) und/oder zu allen Raumbezugspunkten einnehmen,
– dass die Lagen der Mehrheit aller Identitätsräume in bezug auf die Bezugsräume zweier aufeinanderfolgenden Vorgaben gleich bleiben, oder die Lage eines Identitätsraumes in bezug auf die Bezugsräume dreier aufeinanderfolgender Zeitpunkte sich nur ändert.

15. Verfahren nach den Ansprüchen 12, 14 oder 13, 14 dadurch gekennzeichnet, dass der Identitätspunkt als Mehrheitsentscheid aus gleichen zu drei aufeinanderfolgenden Zeitpunkten ermittelten Identitätspunkten gebildet wird.

16. Verfahren nach den Ansprüchen 12, 14 oder 13, 14 dadurch gekennzeichnet, dass der Identitätspunkt als Mehrheitsentscheid von gleichen Identitätspunkten aus zur gleichen Zeit existierenden Identitätsräumen gebildet wird.

17. Verfahren nach Anspruch 1 dadurch gekennzeichnet,
– dass alle Verschlüsselungsräume im globalen Raum jeweils einen eindeutigen Bezug zu allen Bezugsräumen (BR) und/oder zu allen Raumbezugspunkten einnehmen,
– dass die Lagen der Mehrheit aller Verschlüsselungsräume in bezug auf die Bezugsräume zweier aufeinanderfolgenden Vorgaben gleich bleiben, oder die Lage eines Verschlüsselungsraumes in bezug auf die Bezugsräume dreier aufeinanderfolgender Zeitpunkte sich nur ändert.

18. Verfahren nach den Ansprüchen 12, 17 oder 13, 17 dadurch gekennzeichnet, dass der Verschlüsselungs-

punkt als Mehrheitsentscheid aus gleichen zu drei aufeinanderfolgenden Zeitpunkten ermittelten Verschlüsselungspunkten gebildet wird.

19. Verfahren nach den Ansprüchen 12, 17 oder 13, 17 dadurch gekennzeichnet, dass der Verschlüsselungspunkt als Mehrheitsentscheid von gleichen Verschlüsselungspunkten aus zur gleichen Zeit existierenden Verschlüsselungsräumen gebildet wird.

20. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass der Bezugspunkt Punkt des Bezugsraums (BR) ist oder die Bezugspunkte Punkte des Bezugsraumes (BR) sind.

21. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass der Bezugspunkt der Raumbezugspunkt ist, oder die Bezugspunkte die Raumbezugspunkte sind.

22. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass der Empfänger seine Identität anhand mindestens eines Identitätspunktes in bezug auf mindestens einen Identitätsraum und/oder einer Identitätsbezugsfläche und/oder einen Identitätsbezugspunkt ermittelt.

23. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass der Bezugspunkt ein Providerpunkt ist oder die Bezugspunkte mehrere Providerpunkte in einem Providerraum oder mehreren Providerräumen sind, wobei die Providerpunkte einem Providersystem zugeordnet sind.

24. Verfahren nach Anspruch 23 dadurch gekennzeichnet, dass die Lage jedes Providerpunktes im Providerraum durch den Schnittpunkt mindestens zweier Lotgeraden in bezug auf mindestens zweier Providerbezugsebenen bestimmt ist, wobei der Lotpunkt auf der Providerbezugsebene Providerbezugspunkt sei.

25. Verfahren nach Anspruch 24 dadurch gekennzeichnet, dass ein Providerbezugspunkt oder alle Providerbezugspunkte vom Vorgabensender gesendet werden.

26. Verfahren nach den Ansprüchen 2 und 23 dadurch gekennzeichnet, das in mindestens einer Zusatzinformation mindestens ein Providerbezugspunkt von einem Providersystem gesendet wird.

27. Verfahren nach den Ansprüchen 1 und 23 dadurch gekennzeichnet, dass ein Providerbezugspunkt bzw. die Providerbezugspunkte oder der Providerpunkt bzw. die Providerpunkte über eine Service-Provider-Card dem Empfänger und dem Sender mitgeteilt werden.

28. Verfahren nach den Ansprüchen 1 und 23 dadurch gekennzeichnet, dass die Providerbezugspunkte oder die Providerpunkte geheim und nicht manipulierbar in dem Sender und Empfänger gespeichert werden.

29. Verfahren nach Anspruch 28 dadurch gekennzeichnet, dass alle Providerbezugspunkte oder alle Providerpunkte eines Providers auf die Service-Provider-Card gespeichert werden.

30. Verfahren nach den Ansprüchen 1, 4 und 6 dadurch gekennzeichnet, dass alle einer Person zugeordneten geheimen Identitätspunkte und geheimen Identitätsbezugspunkte und der im Empfänger bekannt werdende Identitätspunkt auf einer ID-Card nicht manipulierbar und nicht lesbar gespeichert sind.

31. Verfahren nach den obigen Ansprüchen dadurch gekennzeichnet, dass auf der ID-Card der Identitätsraum, die Lotgeraden, der Schnittpunkt beider Lotgeraden, der für den Austausch vorgesehene geheimen Identitätspunkt, aus einem empfangenen Telegramm, das sogenannte Kartendatentelegramm KDT1, die Kartenbezugspunkte, die Ursprungspunkte zweier Lagen des Verschlüsselungsraumes, der Ursprungspunkt des Identitätsraumes in bezug auf einen globalen Raum, der Verschlüsselungspunkt im Verschlüsselungsraum, die Abstandsvektoren und/oder die Einheitsvektoren aller für den Austausch vorgesehenen Identitätspunkte in bezug auf die Kartenbezugspunkte im globalen Raum ermittelt und die Vektoren in einem Sendetelegramm, das sogenannte Kartendatentelegramm KDT2, gesendet werden.

32. Verfahren nach den Ansprüchen 2 und 31 dadurch gekennzeichnet, dass das Kartendatentelegramm KDT1 in einem ersten Telegrammteil Einheitsvektoren und/oder Abstandsvektoren und in einem zweiten Telegrammteil mindestens die Ortvektoren zweier Lagen des Ursprungspunktes des Verschlüsselungsraumes, des Ursprungspunktes des Identitätsraumes, zweier Kartenbezugspunkte und Zufallszahlen enthält, wobei die Daten im zweiten Telegrammteil in Abhängigkeit von den im Verschlüsselungspunkt enthaltenen Informationen verschlüsselt sind.

33. Verfahren nach Anspruch 32 dadurch gekennzeichnet, dass die Einheitsvektoren Vektoren der Geraden mit den Punkten des Verschlüsselungspunktes und je einem Kartenbezugspunkt im globalen Raum sind.

34. Verfahren nach Anspruch 31 dadurch gekennzeichnet, dass auf der ID-Card die Ortvektoren mindestens zweier zur Berechnung der Einheitsvektoren und/oder Abstandsvektoren benutzten, und zweier zukünftig benutzten Kartenbezugspunkte und die Ortvektoren mindestens eines vorherbenutzten, eines geradbenutzten und eines zukünftig benutzten Ursprungs des Verschlüsselungsraumes gespeichert werden.

35. Verfahren nach Anspruch 34 dadurch gekennzeichnet, dass die ID-Card mit dem vorherbenutzten Ortvektor des Ursprunges des Verschlüsselungsraumes die zur Zeit in Benutzung befindlichen Kartenbezugspunkte anzeigt.

36. Verfahren nach den Ansprüchen 1–3 und 23–29 dadurch gekennzeichnet, dass auf der Service-Provider-Card der Providerraum, die Lotgeraden, die Schnittpunkte der Lotgeraden, die für den Austausch vorgesehenen geheimen Providerpunkte, aus einem empfangenen Telegramm, das sogenannte Provider-Kartendatenempfangstelegramm, die Kartenbezugspunkte, die Ursprungspunkte zweier Lagen des Verschlüsselungsraumes, der Ursprungspunkt des Providerraumes in bezug auf einen globalen Raum, der Verschlüsselungspunkt im Verschlüsselungsraum, die Abstandsvektoren und/oder die Einheitsvektoren aller für den Austausch vorgesehenen Providerpunkte in bezug auf die Kartenbezugspunkte im globalen Raum ermittelt und die Vektoren in einem Sendetelegramm, das sogenannte Provider-Kartendatensendetelegramm, gesendet werden.

37. Verfahren nach den Ansprüchen 2 und 36 dadurch gekennzeichnet, dass das Provider-Kartendatenempfangstelegramm in einem ersten Telegrammteil Einheitsvektoren und/oder Abstandsvektoren und in einem zweiten Telegrammteil mindestens die Ortvektoren zweier Lagen des Ursprungspunktes des Verschlüsselungsraumes, des Ursprungspunktes des Providerraumes, zweier Kartenbezugspunkte und Zufallszahlen enthält, wobei die Daten im zweiten Telegrammteil in Abhängigkeit von den im Verschlüsselungspunkt enthaltenen Informationen verschlüsselt sind.

38. Verfahren nach Anspruch 37 dadurch gekennzeichnet, dass die Einheitsvektoren Vektoren der Geraden mit den Punkten des Verschlüsselungspunktes und je einem Kartenbezugspunkt im globalen Raum sind.

39. Verfahren nach Anspruch 36 dadurch gekenn-

zeichnet, dass auf der Service-Provider-Card die Ortvektoren mindestens zweier zur Berechnung der Einheitsvektoren und/oder Abstandsvektoren benutzten, und zweier zukünftig benutzten Kartenbezugspunkte und die Ortvektoren mindestens eines vorherbenutzten, eines geradbenutzten und eines zukünftig benutzten Ursprungs des Verschlüsselungsraumes gespeichert werden.

40. Verfahren nach Anspruch 39 dadurch gekennzeichnet, dass die Service-Provider-Card mit dem vorherbenutzten Ortvektor des Ursprunges des Verschlüsselungsraumes die zur Zeit in Benutzung befindlichen Kartenbezugspunkte anzeigt.

41. Verfahren nach den Ansprüchen 1–3 dadurch gekennzeichnet, dass der Vorgabensender ein Telegramm, das sogenannte Vorgabendatentelegramm, zum Sender und Empfänger sendet, das in einem ersten Telegrammteil mindestens einen Controllerschlüssel, zwei Einheitsvektoren und/oder Abstandsvektoren, in einem zweiten Telegrammteil mindestens die Ortvektoren zweier Lagen des Ursprungspunktes des Verschlüsselungsraumes, des Ursprungspunktes des Identitätsraumes, zweier Kartenbezugspunkte, zweier Controllerverschlüsselungsbezugspunkte, von sechs globalen Raumbezugspunkten und Zufallszahlen enthält, wobei die Daten im zweiten Telegrammteil in Abhängigkeit von den im Verschlüsselungspunkt enthaltenen Informationen verschlüsselt sind.

42. Verfahren nach Anspruch 41 dadurch gekennzeichnet, dass die Einheitsvektoren Vektoren der Geraden mit den Punkten des Verschlüsselungspunktes und je einem Controllerverschlüsselungsbezugspunkt im globalen Raum sind.

43. Verfahren nach den Ansprüchen 1–21, 30–35, 41 und 42 dadurch gekennzeichnet,

- dass ein Vorgabentelegramm-Schlüssel-Controller eines Telegramm-Schlüssel-Controllers, der aus einem Kartentelegramm-Schlüssel-Controller, einem Vorgabentelegramm-Schlüssel-Controller, einem Datentelegramm-Schlüssel-Controller und aus einer Schlüssel-Protokollierungs-Einheit besteht, den Verschlüsselungspunkt als Schnittpunkt zweier in den Controllerbezugspunkten angetragenen Einheitsvektoren und 1 oder Abstandsvektoren, aus den Koordinaten des Verschlüsselungspunktes den Schlüssel des Vorgabensenders bestimmt und die Daten entschlüsselt, alle Räume und Bezugspunkte ermittelt,
- dass der Kartentelegramm-Schlüssel-Controller bei Sendewunsch unter Kenntnis des gesendeten vorherbenutzten Ursprungs des Verschlüsselungsraums auf der ID-Card die zu benutzenden Kartenbezugspunkte auswählt, den Verschlüsselungspunkt in bezug auf die Kartenbezugspunkte, Zufallszahlen und das Kartendatentelegramm KDT1 generiert sowie aussendet, aus den Vektoren des Kartendatentelegramms KDT2 in bezug auf die Kartenbezugspunkte alle zum Austausch benutzten Identitätspunkte bestimmt,
- dass der Datentelegramm-Schlüssel-Controller den Verschlüsselungspunkt im Verschlüsselungsraum, die Einheitsvektoren oder Abstandsvektoren von allen zu übertragenden Identitätspunkte und Verschlüsselungspunkte zu mehr als einen globalen Raumbezugspunkt bestimmt, die Verschlüsselung der zusendenden Daten entsprechend den Koordinateninformationen des Verschlüsselungsvektors vornimmt und ein Telegramm, das sogenannte Datentelegramm DT2, generiert und aussendet.

44. Verfahren nach Anspruch 43 dadurch gekennzeichnet, dass der Datentelegramm-Schlüssel-Controller aus einem empfangenen Telegramm, das sogenannte Datentelegramm DT1, die Einheitsvektoren oder die Abstandsvektoren, den Verschlüsselungspunkt bzw. die Verschlüsselungspunkte und alle Identitätspunkte aus den Einheitsvektoren oder Abstandsvektoren in bezug auf die globalen Raumpunkte und die Koordinateninformationen des Verschlüsselungspunktes bestimmt.

45. Verfahren nach Anspruch 44 dadurch gekennzeichnet, dass die Zusatzinformationen aus den verschlüsselten Daten bestimmt und ausgewertet werden.

46. Verfahren nach Anspruch 45 dadurch gekennzeichnet, dass die verschlüsselten Daten auf einem Datenspeicher gespeichert werden.

47. Verfahren nach Anspruch 46 dadurch gekennzeichnet, dass die Daten nur bei der Benutzung und für die Benutzung entschlüsselt werden.

48. Verfahren nach Anspruch 45 dadurch gekennzeichnet, dass in einer Schlüssel-Protokollierungs-Einheit mindestens der Verschlüsselungspunkt und/oder der geheime Identitätspunkt und/oder der bekannt werdende Identitätspunkt und/oder Gültigkeitszeitraum des Verschlüsselungspunktes und/oder die Art der Daten anhand einer Datentelegrammverwaltungsnummer gespeichert werden.

49. Verfahren nach Anspruch 48 dadurch gekennzeichnet, dass nach Ablauf des Gültigkeitszeitraumes der Verschlüsselungspunkt gelöscht wird.

50. Verfahren nach Anspruch 36 dadurch gekennzeichnet, dass im Telegramm-Schlüssel-Controller die Providerpunkte ermittelt und alle Kommunikationen mit dem Providersystem in bezug auf die Providerpunkte ausgeführt werden.

51. Verfahren nach den Ansprüchen 7 und 8 dadurch gekennzeichnet, dass mit dem beim Empfänger bekannt werdenden Identitätspunkt die personenbezogene Adresse von einer Adressen-CD ermittelt wird.

52. Verfahren nach Anspruch 51 dadurch gekennzeichnet, dass im Empfänger die Gültigkeit der personenbezogenen Adresse in bezug auf den geheim gespeicherten geheimen Identitätspunkt bestimmt wird.

53. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass der Vorgabensender eine Zentrale ist, der Vorgaben über einen Satelliten sendet.

54. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die Sender und Empfänger über einen zweiten Übertragungsweg kommunizieren.

55. Verfahren nach Anspruch 54 dadurch gekennzeichnet, dass der Übertragungsweg das Internet ist.

Hierzu 11 Seite(n) Zeichnungen

Nummer: **DE 100 43 310 A1**
Int. Cl.[7]: **H 04 L 9/32**
Offenlegungstag: 22. März 2001

Fig. 1

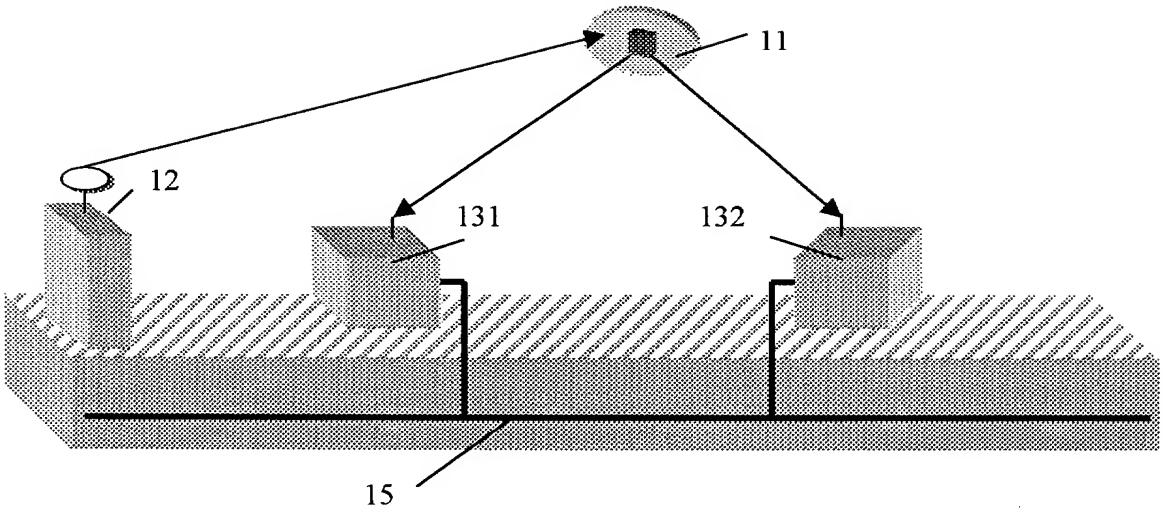
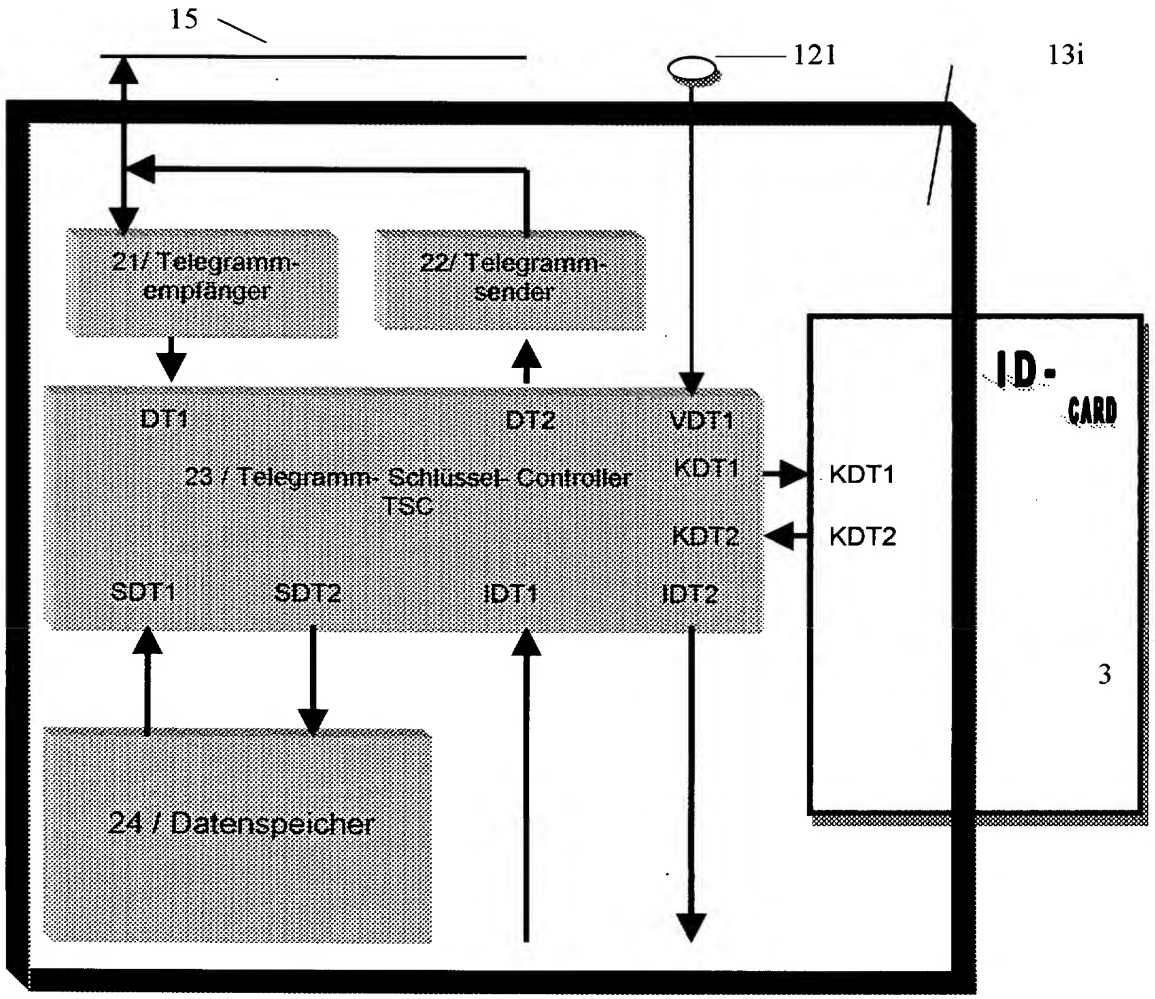
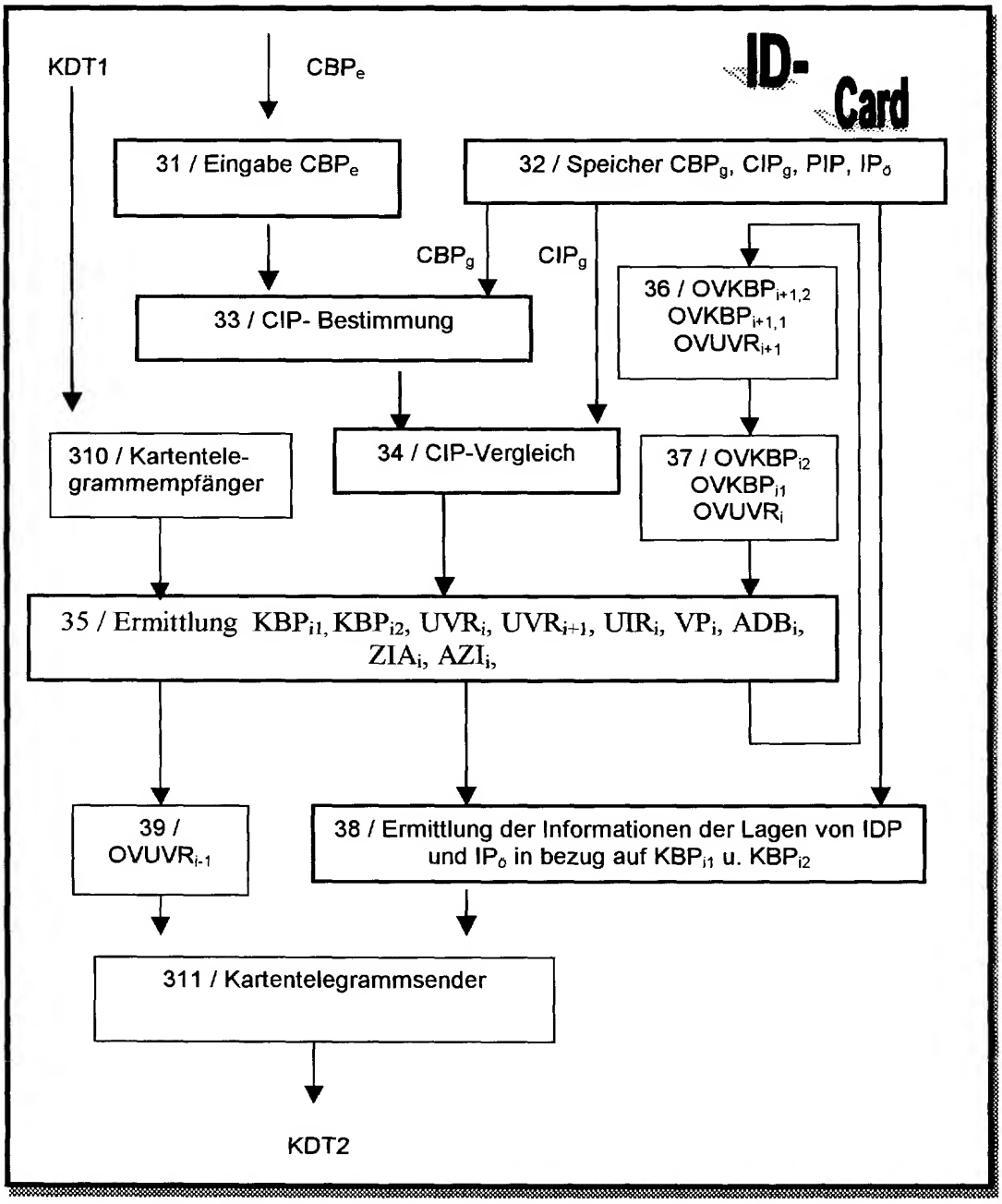


Fig. 2



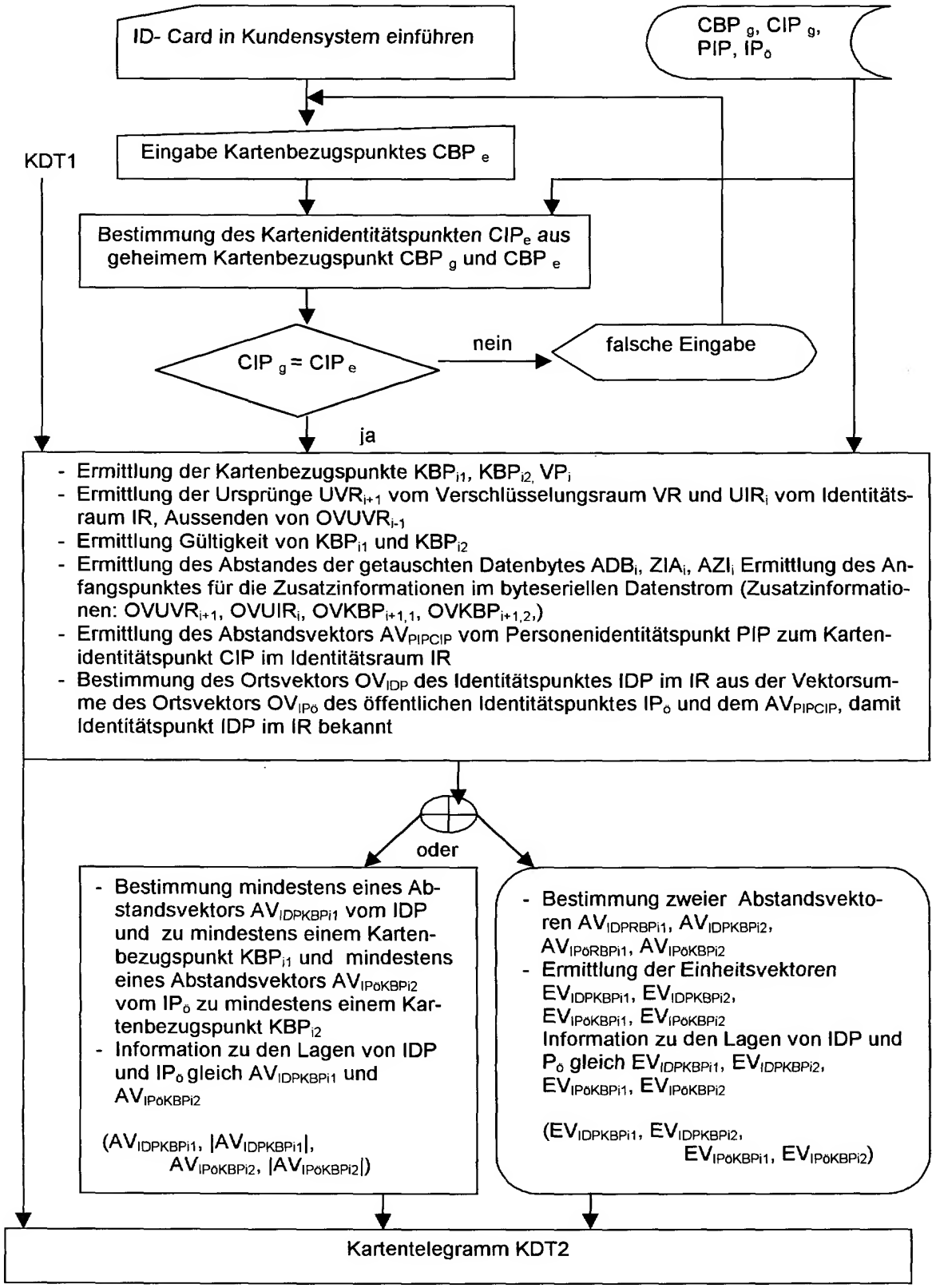
Nummer: DE 100 43 310 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 22. März 2001

Fig. 3



Nummer: **DE 100 43 310 A1**
Int. Cl.[7]: **H 04 L 9/32**
Offenlegungstag: 22. März 2001

Fig. 4 : Verfahrensschritte auf der ID- Card



Nummer: **DE 100 43 310 A1**
Int. Cl.[7]: **H 04 L 9/32**
Offenlegungstag: 22. März 2001

Fig. 5: Aufbau des Kartendatentelegramms KDT1

Einheitsvektor $EV_{VPKBPi1}$	Einheitsvektor $EV_{VPKBPi2}$	VP definierte Vertauschung der Datenbytes mit $OVUVR_i$, $OVUIR_i$, $OVKBP_{i1}$, $OVKBP_{i2}$ und $OVUVR_{i+1}$, Zufallszahlen Z_{si}

◄— Telegrammteil1 —►	◄———— Telegrammteil 2 ————►

Fig. 6: Verfahrensschritte Datenaustausch im Telegrammteil 2

ADB_i - Datenabstand für den Datentausch
ZIA_i - Zusatzinformationsanfangspunkt
AZI_i - Datenabstand der Zusatzinformation
Z_{sk} - Zufallszahl der Sendung s, wobei für jede Sendung andere Zufallszahlen vom Zufallsgenerator gebildet werden

Beispiel:

ADB_i = 5
ZIA_i = 12
AZI_i = 3

Normale Byte-folge	1 $OVUVR_i$	2 $OVUIR_i$	3 $OVKBP_{i1}$	4 $OVKBP_{i2}$	5 $OVUVR_{i+1}$	6 Z_{s1}	7 Z_{s2}	8 Z_{s3}
Verschlüsselte Bytefolge	Z_{s1}	Z_{s2}	Z_{s3}	Z_{s4}	Z_{s5}	Z_{s6}	Z_{s7}	Z_{s8}

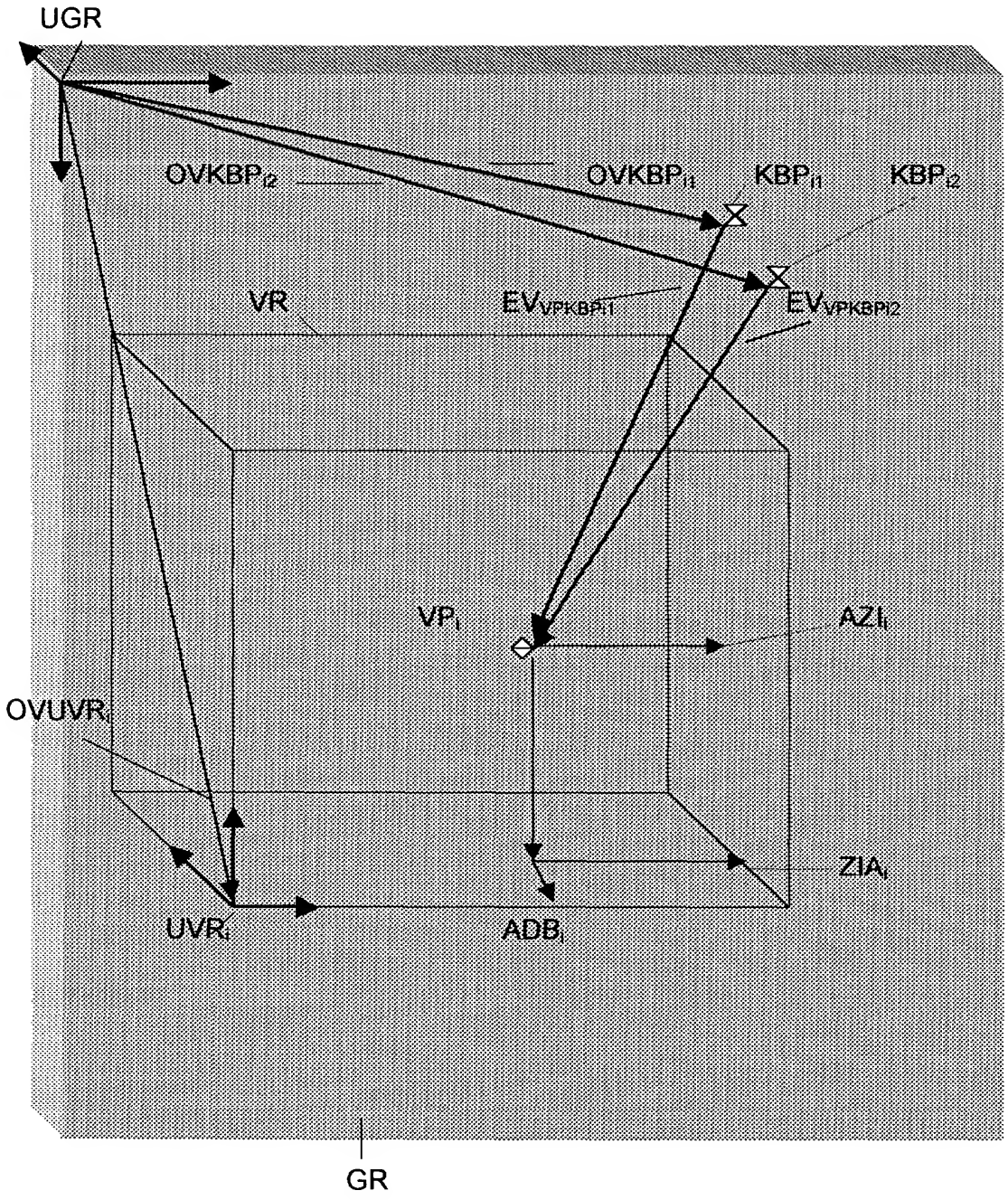
9	10	11	12	13	14	15	16	17	18	19	20
Z_{s4}	Z_{s5}	Z_{s6}	Z_{s7}	Z_{s8}	Z_{s9}	Z_{s110}	Z_{s111}	Z_{s112}	Z_{s113}	Z_{s114}	Z_{s115}
Z_{s9}	Z_{s110}	Z_{s111}	$OVUVR_i$	Z_{s112}	Z_{s113}	$OVUIR_i$	Z_{s114}	Z_{s115}	$OVKBP_{i1}$	Z_{s116}	Z_{s117}

21	22	23	24	25	26	27	28	29	30	31
Z_{s116}	Z_{s117}	Z_{s118}	Z_{s119}	Z_{s120}	Z_{s121}	Z_{s122}	Z_{s123}	Z_{s124}	Z_{s125}	Z_{s126}
$OVKBP_{i2}$	Z_{s118}	Z_{s119}	$OVUVR_{i+1}$	Z_{s120}	Z_{s121}	Z_{s122}	Z_{s123}	Z_{s124}	Z_{s125}	Z_{s126}

usw.

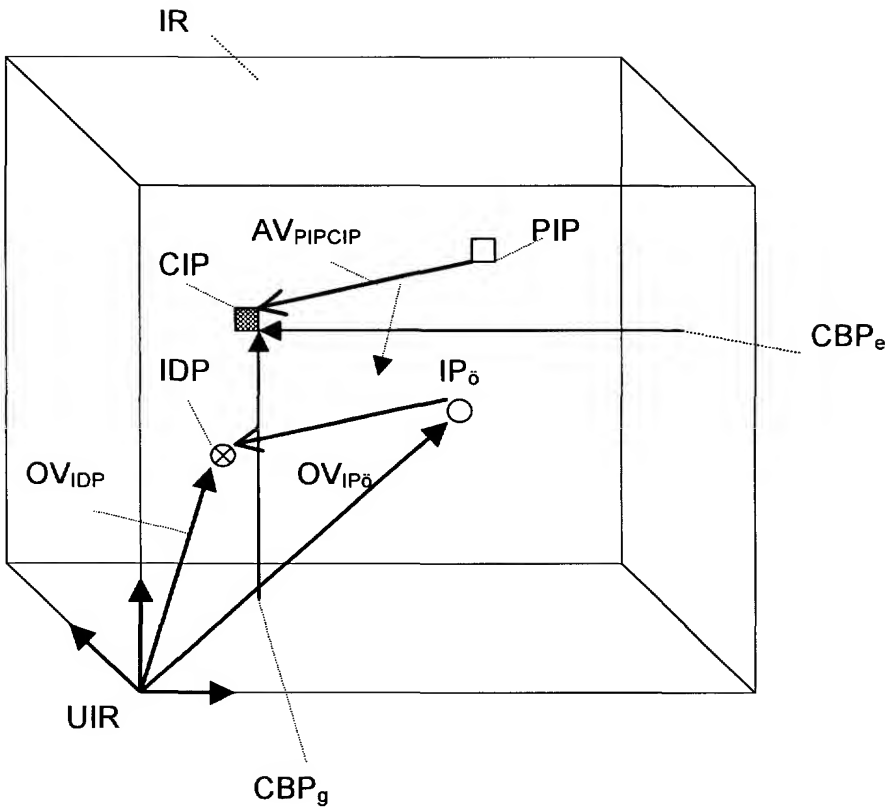
Nummer: **DE 100 43 310 A1**
Int. Cl.[7]: **H 04 L 9/32**
Offenlegungstag: 22. März 2001

Fig. 7



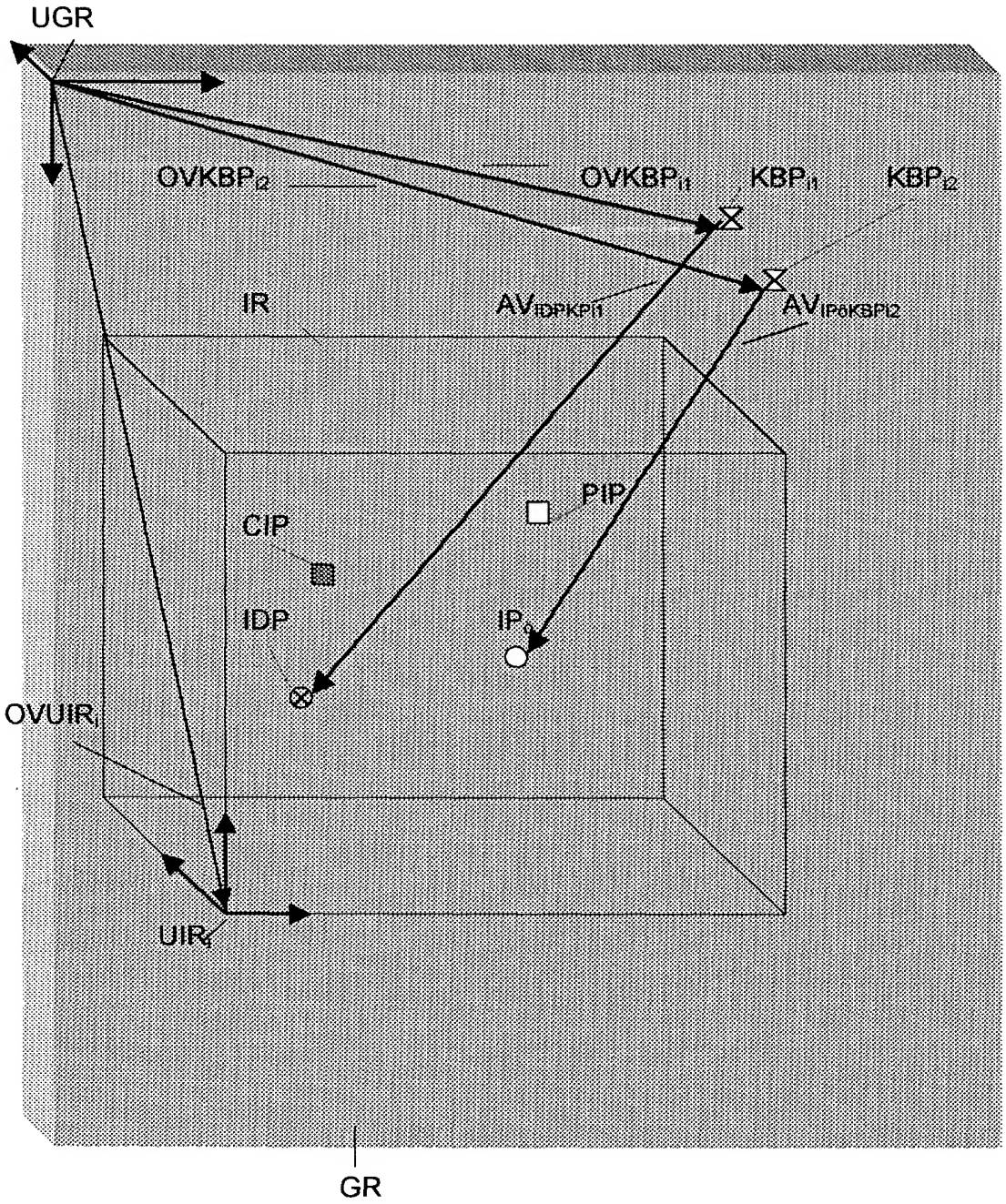
Nummer: **DE 100 43 310 A1**
Int. Cl.[7]: **H 04 L 9/32**
Offenlegungstag: 22. März 2001

Fig. 8



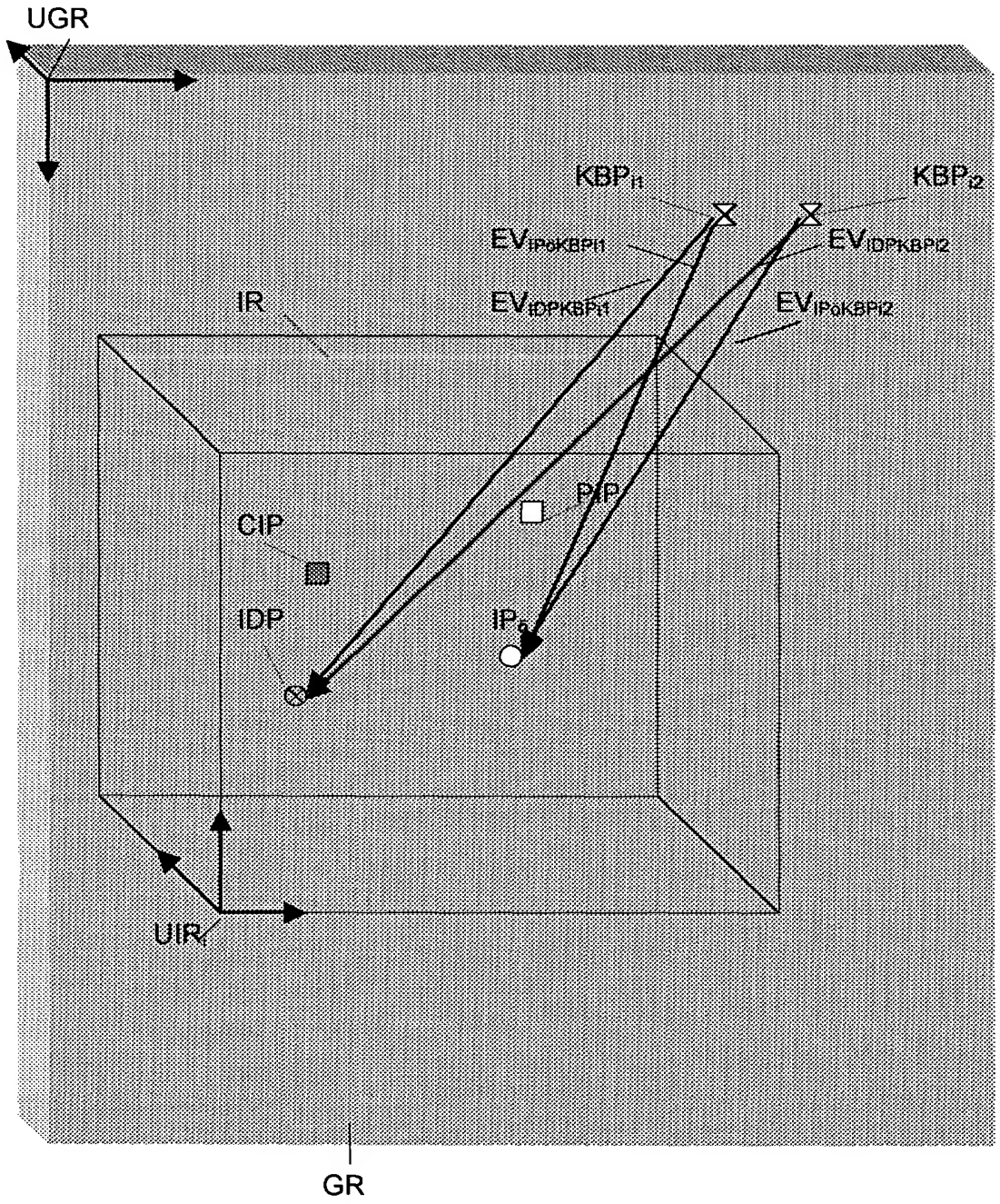
Nummer: DE 100 43 310 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 22. März 2001

Fig. 9



Nummer: **DE 100 43 310 A1**
Int. Cl.[7]: **H 04 L 9/32**
Offenlegungstag: 22. März 2001

Fig. 10



Nummer: **DE 100 43 310 A1**
Int. Cl.[7]: **H 04 L 9/32**
Offenlegungstag: 22. März 2001

Fig. 11: Aufbau des Kartendatentelegramms KDT2

EV - *E*inheitsvektor
$OVUVR_{i-1}$ - Ortvektor des Ursprungs

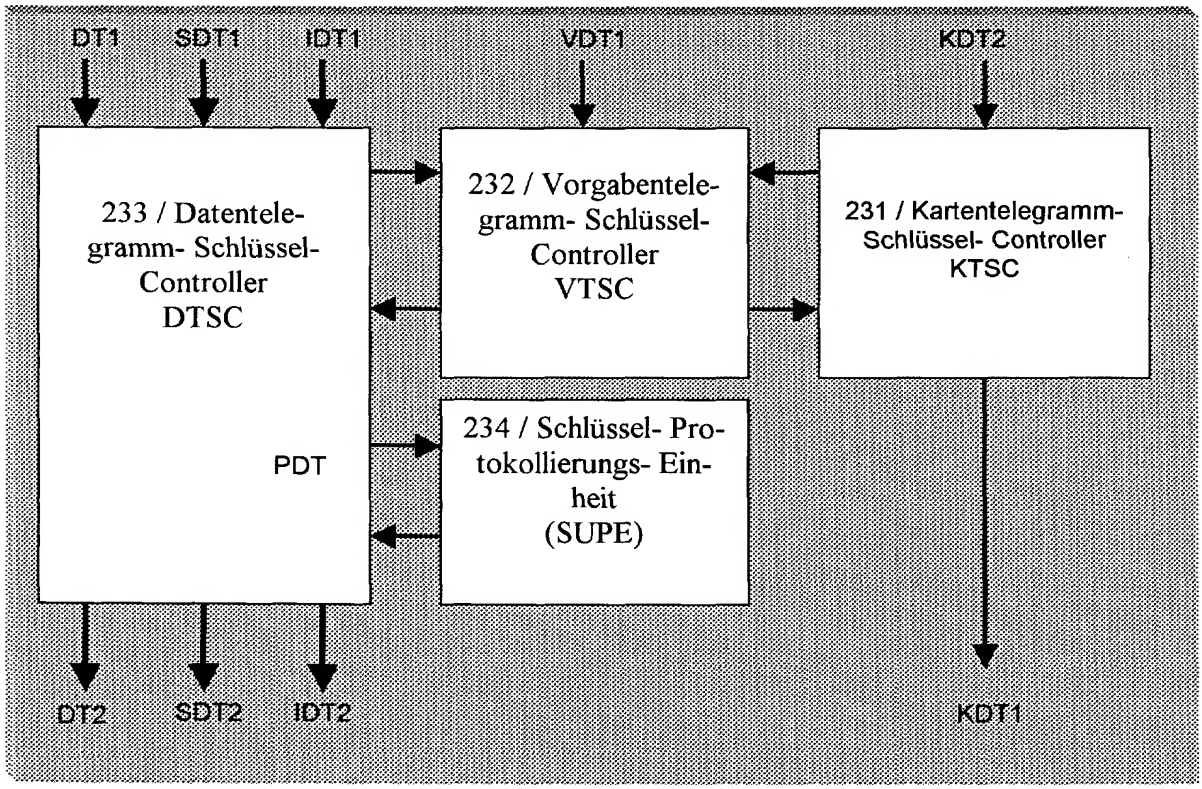
$OVUVR_{i-1}$	$EV_{IDPKBPi1}$	$EV_{IDPKBPi2}$	$EV_{IPöKBPi1}$	$EV_{IPöKBPi2}$

alternativer Verfahrensschritt

AV - *A*bstandsvektor
|AV| - Betrag von AV

$OVUVR_{i-1}$	$AV_{IDPKBPi1}$	$\lvert AV_{IDPKBPi1} \rvert$	$AV_{IPöKBPi2}$	$\lvert AV_{IPöKBPi2} \rvert$

Fig. 12: Telegramm- Schlüssel-Controller (TSC)



Nummer: DE 100 43 310 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 22. März 2001

Fig. 13: Aufbau des Vorgabendatentelegramms VDT1

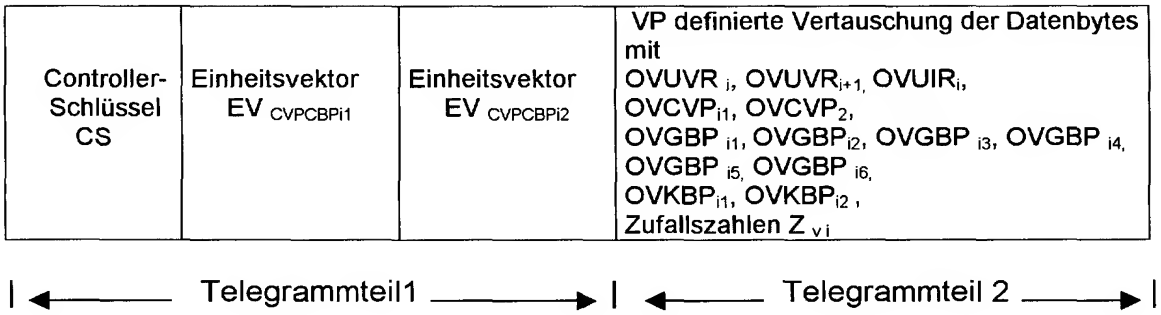


Fig. 14: Aufbau der Datentelegramme DT1 und DT2 - erste Ausführungsart

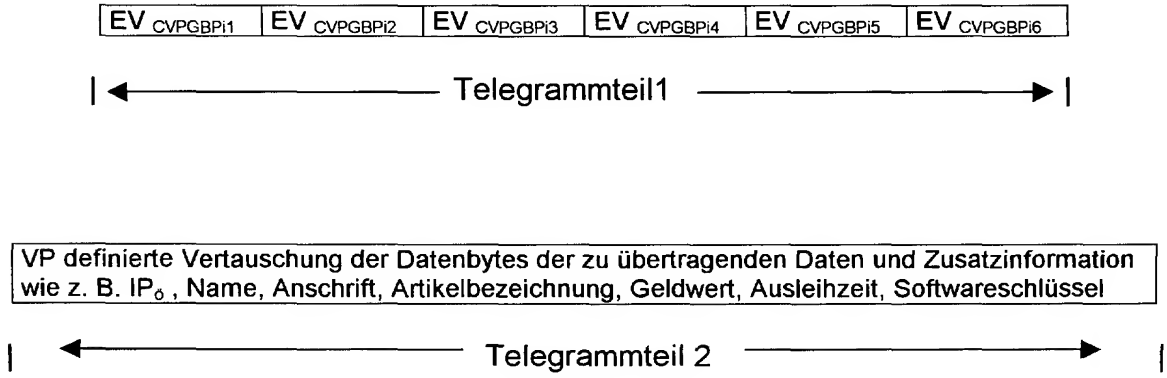
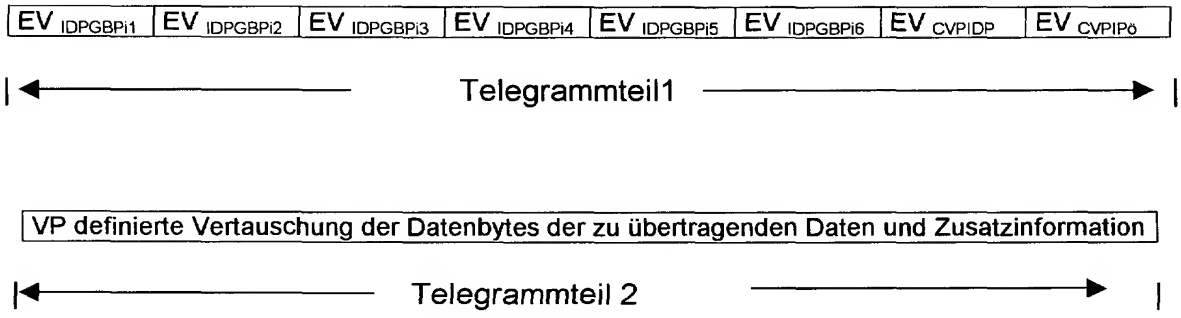


Fig. 15: Aufbau der Datentelegramme DT1 und DT2 - 2. Ausführungsart



Nummer: DE 100 43 310 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 22. März 2001

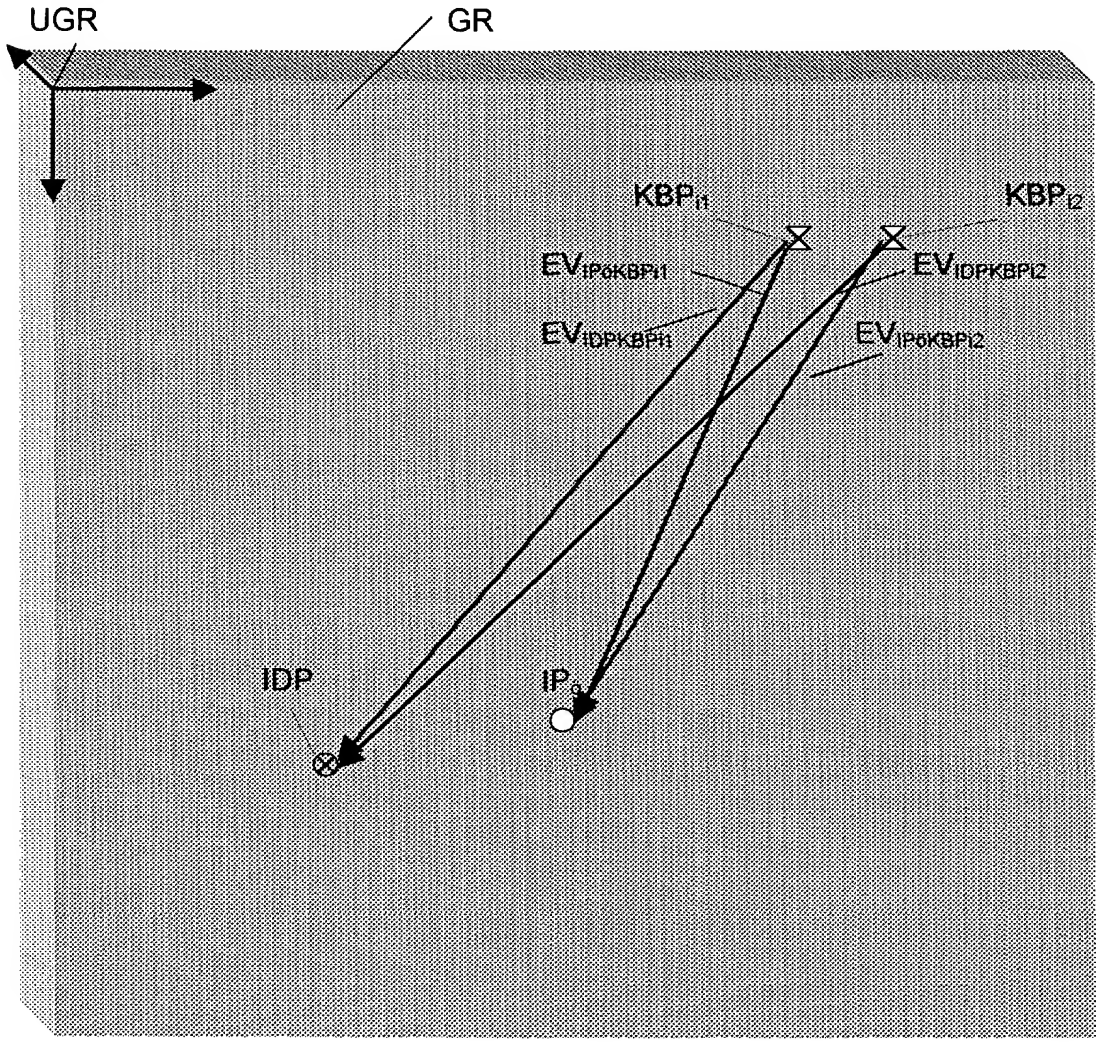
Fig. 16: Aufbau der Speicherdatentelegramme SDT1, SDT2

$DTLN_j$	DB_5	DB_6	DB_1	DB_2	.....	.....		

$DTLN_j$ - Datentelegrammverwaltungsnummer j

DB_k - Datenbyte k entsprechend Verschlüsselungspunkt vertauscht

Fig. 17: Bestimmung von IDP und $IP_ö$ imTSC



DERWENT-ACC-NO: 2001-399144

DERWENT-WEEK: 200143

TITLE: Forgery-proof delivery of electronic data over communications network, changing used standard at random, non-predicable times

INVENTOR: ROZEK W

PATENT-ASSIGNEE: ROZEK W[ROZEI]

PRIORITY-DATA: 2000DE-1043310 (August 17, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
DE 10043310 A1	March 22, 2001	DE

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
DE 10043310A1	N/A	2000DE-1043310	August 17, 2000

INT-CL-CURRENT:

TYPE	IPC DATE

CIPS G07F7/10 20060101

ABSTRACTED-PUB-NO: DE 10043310 A1

BASIC-ABSTRACT:

NOVELTY - The method involves transmitting electronic data from a transmitter to a receiver over communications networks, whereby a global space, an identity space, identity reference points, identity points, an encryption point, and spatial reference points are available. An used standard is changed at random, non-predicable times. The transmitters and receivers generate spaces, reference areas, and reference points from the standards, determine an identity of a space with respect to its identity points, determine information concerning the positions of the identity points and of an encryption point with respect to reference points.

USE - In communications network, e.g. internet.

ADVANTAGE - Assures unique and forgery-proof identification of client.

TITLE-TERMS: FORGE PROOF DELIVER ELECTRONIC DATA COMMUNICATE NETWORK CHANGE STANDARD RANDOM NON TIME

DERWENT-CLASS: T01 W01

EPI-CODES: T01-D01; T01-H01C2; T01-H07C; T01-J12C; W01-A05A; W01-A06B7;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: 2001-294114